International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 03 | Mar 2020 www.irjet.net p-ISSN: 2395-0072

# Privacy Preserving Keyword Search over Encrypted Data in the Cloud

**D. VETRISELVI[1], N.M. JAYASHRI[2]**

*[1]Assistant Professor Deptartment of Computer Science and Engineering Jeppiaar SRR Engineering College, Padur Chennai, Tamil Nadu, INDIA*
*[2]B.E Department of Computer Science and Engineering Jeppiaar SRR Engineering College, Padur Chennai, Tamil Nadu, INDIA*

---

**Abstract -** *Research in cloud computing is receiving tons of attention from both academic and industrial worlds. Clouds can provide several kind of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g.,Amazon's EC2, Eucalyptus, Nimbus), and platforms to assist developers write applications(e.g., Amazon's S3, Windows Azure). Much of the info stored in clouds is very sensitive, for instance , medical records and social networks. Security and privacy are thus vital issues in cloud computing. The user should authenticate itself before beginning any transaction. It must be ensured that the cloud doesn't tamper with the data that is out sourced.In order to search in cloud, some requirements is needed, search over encrypted data should support the following three functions. In one hand, the searchable encryption schemes support keyword search, and supply an equivalent user experience as searching in Google search with different keywords; single-keyword search is way from satisfactory by only returning very limited and inaccurate search results.,The search user would typically prefer cloud servers to sort the returned search leads to a relevance-based order ranked by the relevance of the search request to the documents.*

***Key Words***: Efficient Revocation, Ciphertext Policy Attribute Based Encryption, Standard Model

## 1. INTRODUCTION

Mobile cloud computing has been detailed as a key enabling technology to overcome the physical limit of mobile devices towards scalable and flexible mobile services. In the mobile cloud environment searchable encryption, which allows precisely search over encrypted data, is a key technique to maintain both the privacy and availableof outsourced data in cloud. On addressing the hardness , many research efforts resolve to using the searchable symmetric encryption (SSE) and searchable public-key encryption (SPE). By giving thorough security analysis, we demonstrate that PSU are able to do a high security level. Using extensive experiments during a realworld mobile environment, we show that PUS is more efficient compared with the prevailing proposals.

### 1.1 Proposed system

In Proposed system, PSU (personalized search) scheme with efficient and secure updates we introduced an efficient and reliable methodology for search over encrypted data.Here the encrypted keyword search pre computes the resulting hunt documents for the input query from users through Natural language processing Technique which is carry out on gateway (client side) on user file upload. Hence the matching documents which is pre compute the before arching the encrypted cloud contents are retrieved from cloud. Here we does not pull all the encrypted data's from cloud for searching, which is time consuming and inadequate. The matching documents memory locations on mobile storage are restore from the serializable objects which is reserved in the gateway. User can download the produced documents after getting the keys from the group owner. Asymmetric kind of encryption for key re-encryption and is more assured.

## 2. TECHNOLOGIES USED

### a) Cloud Computing

Cloud computing may be a sort of computing during which dynamically scalable and sometimes virtualities resources are provided as a service over the web .Users needn't have knowledge of, skills in, or control over the technology infrastructure within the "cloud" that supports them. The concept generally conditions combinations of infrastructureas a service (IaaS), platform as a service (PaaS), software as a service (SaaS).Cloud computing customers do not commonly own the physical infrastructure. serving as host to the software platform in question. Instead, they avoid capital expenditure by renting usage from a third-party provider.Cloud computing is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the web .Users needn't have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. The concept generally incorporates combinations of infrastructure as a service (IaaS) ,platform as a service (PaaS) ,software as a service (SaaS).

### b)JAVA

It is a Platform Independent. Java is an object-oriented programming language matured initially by James Gosling and colleagues at Sun Microsystems. The language, initially called Oak (named after the oak trees outside Gosling's office), was proposed to replace C++, although the feature set better feature that of Objective C.

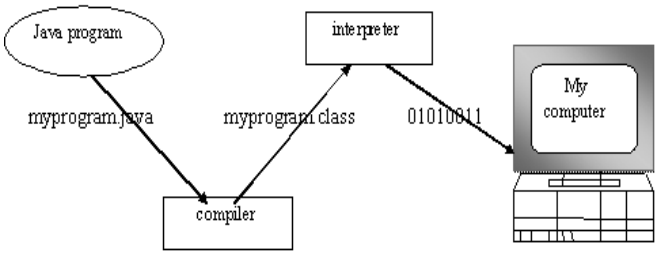



**Fig -1**: WORKING OF JAVA

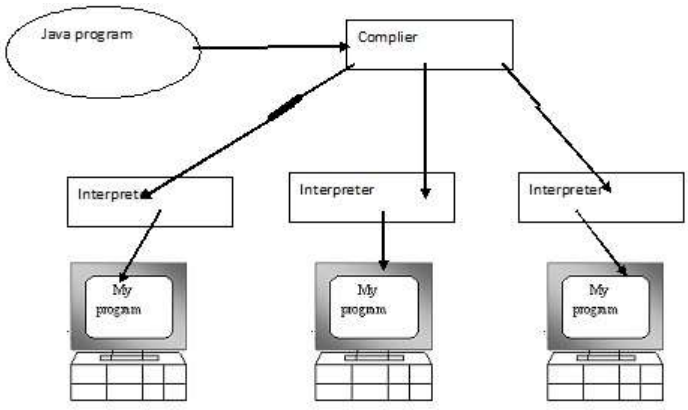



**Fig -2**: JAVA

**c) APACHE TOMCAT SERVER**

Apache Tomcat is a web package developed at the Apache Software Foundation. Tomcat appliance the servlet and the JavaServer Pages (JSP) detail item particularization from Sun Microsystems, providing an environment for Java code to run in cooperation with a web server. It adds tools for configuration and management but can also be construct by editing configuration files that are normally XML -formatted. Because Tomcat includes its own HTTP server privately, it is also considered a standalone web server.

**3. MODULES**

The System is categorized into following modules:

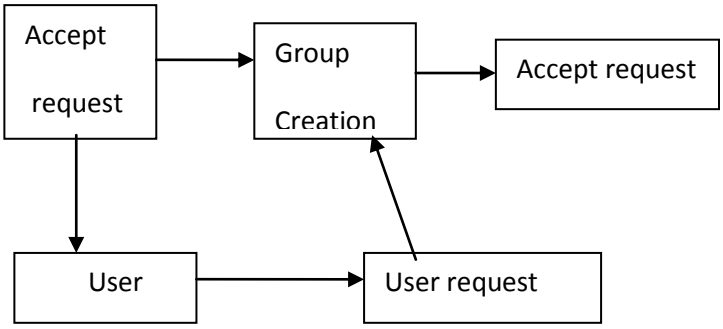
1) Group creation

2) Text Mining process

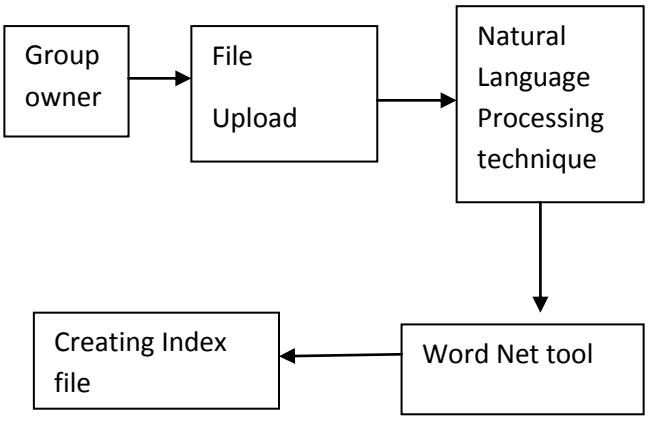
3) Blind storage

4) Query search

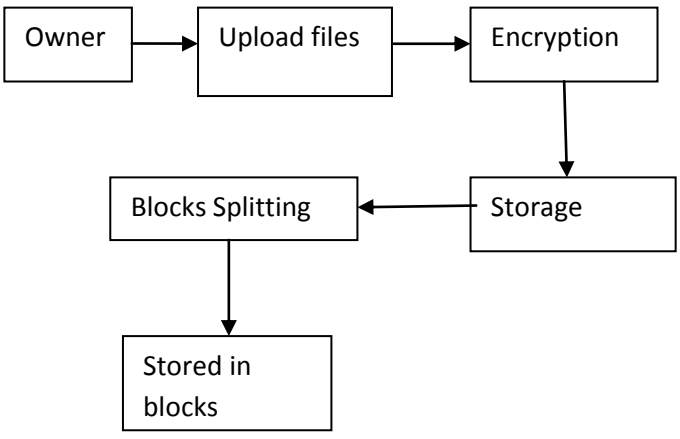
**1) GROUP CREATION**: Data owner should be registered in this environment and create a group. Data users also registers and give request to group owner to add a group user. Data owner accept the request from the user.



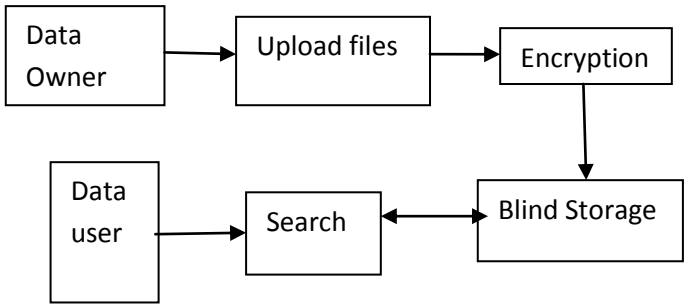

**2) TEXT MINNING PROCESS**: In this module the data owner can upload the documents. Data owner can upload the files, the content of file is to be separated using NLP technique and that words can get synonyms using Word Net tool.



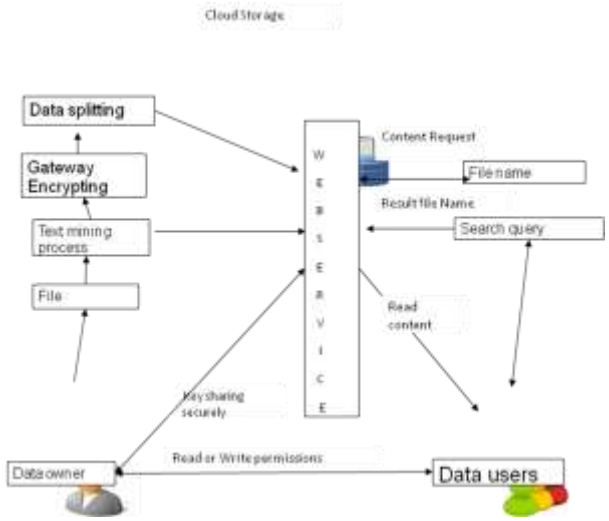

**3) BLIND STORAGE:** The uploaded data's are encrypted in gateway after Natural language Processing is done and saved as index file. The owner can give access control and authority to user while uploading the data.




**4) QUERY SEARCH**: Data user will try to haunt a query in cloud server. The cloud servers plot relief map the keywords and search the related files.




## 4. Architecture Diagram




## 5. Conclusion

Hence we developed an efficient search in keyword through updates which enable accurate, efficient and secure search over encrypted data. Privacy is preserved for data in cloud while storing in blind Storage, and also manage approach control for each user.

### 6. Enhancement

- Multiple group creation, each group is having owner and multiple users.
- Multimedia Search.
- To encrypt data using Asymmetric algorithm (RSA) and key re-encryption.
- Using NLP technique and word net tool for text mining process.
- Index file and Key generation on cloud.

### REFERENCES

[1] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Y. Luo, ‘‘Exploiting geo-distributed clouds for a E-health monitoring system with minimum ser-vice delay and privacy preservation,’’ IEEE J. Biomed. Health Informat., vol. 18, no. 2, pp. 430–439, Mar. 2014. VOLUME 6, NO. 1, MARCH 2018 107 IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING Li et al.: Personalized Search Over Encrypted Data With Efficient and Secure Updates

[2] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, ‘‘An SMDP-based service model for interdomain resource allocation in mobile cloud networks,’’ IEEE Trans. Veh. Technol., vol. 61, no. 5, pp. 2222–2232, Jun. 2012.

[3] Y. Cai, F. Yu, and S. Bu, ‘‘Cloud computing meets mobile wireless com-munications in next generation cellular networks,’’ IEEE Netw., vol. 28,no. 6, pp. 54–59, Nov./Dec. 2014.

[4] D. Zeng, S. Guo, I. Stojmenovic, and S. Yu, ‘‘Stochastic modeling and analysis of opportunistic computing in intermittent mobile cloud,’’ in Proc. 8th IEEE Conf. Ind. Electron. Appl. (ICIEA), Jun. 2013, pp. 1902–1907.

[5] S. Yu, R. Doss, W. Zhou, and S. Guo, ‘‘A general cloud firewall framework with dynamic resource allocation,’’ in Proc. ICC, Jun. 2013, pp. 1941–1945.

[6] F. R. Yu and V. Leung, Advances in Mobile Cloud Computing Systems. Boca Raton, FL, USA: CRC Press, 2015.